



OMA DRM Requirements

Candidate Version 2.2 – 29 June 2010

Open Mobile Alliance
OMA-RD-DRM-V2_2-20100629-C

Use of this document is subject to all of the terms and conditions of the Use Agreement located at <http://www.openmobilealliance.org/UseAgreement.html>.

Unless this document is clearly designated as an approved specification, this document is a work in process, is not an approved Open Mobile Alliance™ specification, and is subject to revision or removal without notice.

You may use this document or any part of the document for internal or educational purposes only, provided you do not modify, edit or take out of context the information in this document in any manner. Information contained in this document may be used, at your sole risk, for any purposes. You may not use this document in any other manner without the prior written permission of the Open Mobile Alliance. The Open Mobile Alliance authorizes you to copy this document, provided that you retain all copyright and other proprietary notices contained in the original materials on any copies of the materials and that you comply strictly with these terms. This copyright permission does not constitute an endorsement of the products or services. The Open Mobile Alliance assumes no responsibility for errors or omissions in this document.

Each Open Mobile Alliance member has agreed to use reasonable endeavours to inform the Open Mobile Alliance in a timely manner of Essential IPR as it becomes aware that the Essential IPR is related to the prepared or published specification. However, the members do not have an obligation to conduct IPR searches. The declared Essential IPR is publicly available to members and non-members of the Open Mobile Alliance and may be found on the "OMA IPR Declarations" list at <http://www.openmobilealliance.org/ipr.html>. The Open Mobile Alliance has not conducted an independent IPR review of this document and the information contained herein, and makes no representations or warranties regarding third party IPR, including without limitation patents, copyrights or trade secret rights. This document may contain inventions for which you must obtain licenses from third parties before making, using or selling the inventions. Defined terms above are set forth in the schedule to the Open Mobile Alliance Application Form.

NO REPRESENTATIONS OR WARRANTIES (WHETHER EXPRESS OR IMPLIED) ARE MADE BY THE OPEN MOBILE ALLIANCE OR ANY OPEN MOBILE ALLIANCE MEMBER OR ITS AFFILIATES REGARDING ANY OF THE IPR'S REPRESENTED ON THE "OMA IPR DECLARATIONS" LIST, INCLUDING, BUT NOT LIMITED TO THE ACCURACY, COMPLETENESS, VALIDITY OR RELEVANCE OF THE INFORMATION OR WHETHER OR NOT SUCH RIGHTS ARE ESSENTIAL OR NON-ESSENTIAL.

THE OPEN MOBILE ALLIANCE IS NOT LIABLE FOR AND HEREBY DISCLAIMS ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF DOCUMENTS AND THE INFORMATION CONTAINED IN THE DOCUMENTS.

© 2010 Open Mobile Alliance Ltd. All Rights Reserved.

Used with the permission of the Open Mobile Alliance Ltd. under the terms set forth above.

Contents

1. SCOPE (INFORMATIVE)	5
2. REFERENCES	6
2.1 NORMATIVE REFERENCES	6
2.2 INFORMATIVE REFERENCES	6
3. TERMINOLOGY AND CONVENTIONS	7
3.1 CONVENTIONS	7
3.2 DEFINITIONS	7
3.3 ABBREVIATIONS	8
4. INTRODUCTION (INFORMATIVE)	10
4.1 VERSION 2.2	10
5. DRM 2.2 RELEASE DESCRIPTION (INFORMATIVE)	11
6. MARKET REQUIREMENTS	12
7. ENGINEERING REQUIREMENTS	16
7.1 SECURITY	16
7.2 CHARGING	18
7.3 STREAMING	19
7.4 SUPERDISTRIBUTION	20
7.5 STORAGE AND BACKUP	20
7.6 RIGHTS	21
7.7 DOMAINS	22
7.8 PRIVACY	22
7.9 ERROR HANDLING	23
7.10 ADMINISTRATION AND CONFIGURATION	24
7.11 TERMINAL DEVICES AND SMARTCARDS	24
7.11.1 Terminal Devices	24
7.11.2 Smartcards	24
7.11.3 Removable Media Cards	24
7.12 PLATFORMS	24
7.13 NETWORK INTERFACES	24
7.14 USABILITY	24
7.15 DRM CONTENT	25
7.16 INTEROPERABILITY AND BACKWARD COMPATIBILITY	25
APPENDIX A. CHANGE HISTORY (INFORMATIVE)	27
A.1 APPROVED VERSION HISTORY	27
A.2 DRAFT/CANDIDATE VERSION DRM 2.2 HISTORY	27
APPENDIX B. USE CASES (INFORMATIVE)	29
B.1 ENFORCED ADVERTISEMENT PLAYBACK	29
B.1.1 Short Description	29
B.1.2 Market benefits	29
B.2 PURCHASE WITHIN AN APPLICATION	29
B.2.1 Short Description	29
B.2.2 Market benefits	30
B.3 VARIABLE BITRATES STREAMING	30
B.3.1 Short Description	30
B.3.2 Market benefits	30
B.4 VIDEO STREAMING: MAXIMUM RESOLUTION & SECURE PATH	30
B.4.1 Short Description	30
B.4.2 Market benefits	31

B.5	RESTRICTION ON NUMBER OF PLAYER DEVICES.....	31
B.5.1	Short Description	31
B.5.2	Market benefits	31
APPENDIX C.	DRM 2.1 USAGE SCENARIOS (INFORMATIVE)	32

1. Scope

(Informative)

This document defines the requirements for the 2.1 release of DRM specification within OMA.

Whereas the aim for DRM v2.0 was to improve the level of security of OMA DRM Version 1, due to the lack of a key management infrastructure, DRM v2.1 will focus on introducing new features based on market feedback:

- A metering capability
- Improvements of (P)DCF file formats linked to user experience (additional Metadata boxes)
- A possibility to identify a device from servers other than those of Rights Issuers
- A binary format for ROAP triggers
- A capability to distinguish between different content categories (ring-tones vs. music tracks, ...), & a clarified support for CD burning

The 2.1 version will also clarify or correct some inconsistencies of the 2.0 version.

Requirements in this document are requirements for Versions 1.0, 2.0 & 2.1 implementations. Requirements are backward compatible, i.e. requirements applying for a given version of the DRM apply to the higher versions, unless stated otherwise.

Unless explicitly stated otherwise, all requirements listed in this document will apply to all platforms (including PC).

2. References

2.1 Normative References

- [RFC2119] "Key words for use in RFCs to Indicate Requirement Levels". S. Bradner. March 1997. <http://www.ietf.org/rfc/rfc2119.txt>
- [3GPP PSS] Transparent end-to-end packet switched streaming service (PSS); 3GPP 26.234; Protocols and codecs - Release 5. <http://www.3gpp.org/>
- [BT AVDTP] Bluetooth Audio/Video Distribution Transport Protocol, Version 1.00
- [BT AVCTP] Bluetooth Audio/Video Control Transport Protocol, Version 1.00
- [BT GAVDP] Bluetooth Generic Audiovisual Distribution Profile, Version 1.00
- [XBS-v1.0] "OMA DRM v2.0 Extensions for Broadcast Support", version 1.0, Open Mobile Alliance™, OMA-TS-DRM_XBS-V1_0, URL: <http://www.openmobilealliance.org/>
- [DRM-v2.1-DRM-TS] "OMA DRM v2.1 DRM Specification ", version 1.0, Open Mobile Alliance™, OMA-TS-DRM_DRM-V2_1, URL: <http://www.openmobilealliance.org/>

2.2 Informative References

- [ISO 7498-2] ISO/IEC 7498: Information processing systems -- Open Systems Interconnection -- Basic Reference Model - Part 2: Security Architecture

3. Terminology and Conventions

3.1 Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

All sections, except appendices, "Scope", and "Introduction" are normative, unless they are explicitly indicated to be informative.

3.2 Definitions

Advertisement Impression Data	Information about the completed advertisement consumption by the user (e.g., number of advertisement playout).
Backup	Defines an action for duplicating a Media Object and/or Rights Object and transferring them to another location that is not a Device.
Billing Service Provider	The entity responsible for collecting payment from a User.
Combined Delivery	A Version 1 method for delivering DRM Content and Rights Object. The Rights Object and DRM Content are delivered together in a single entity, the DRM Message.
Composite Object	A Media Object that contains one or more Media Objects by means of inclusion e.g. DRM messages, zip files.
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals, entities or processes. (From [ISO 7498-2])
Constraint	A restriction on the permission over DRM Content.
Content	One or more Media Objects.
Content Issuer	The entity making content available to the DRM Agent; the entity whose Content is being Protected.
Content Provider	An entity that is either a Content Issuer or a Rights Issuer.
Content subscription	A subscription that a User has with a Content Provider for the purposes of paying for DRM Content purchased from that Content Provider and played on a Users Device.
Copy	To make a perfect reproduction of DRM Content or a Rights Object.
Device	A Device is the entity (hardware/software or combination thereof) within a user equipment that implements a DRM Agent. The Device is also conformant to the OMA DRM Version 2 specifications The Device may include a smartcard module (e.g. a SIM) or not depending upon implementation.
Domain	A group of Devices defined by a Rights Issuer such that the Rights Issuer can issue Rights Objects for the group that can be processed by all Devices within the group, and only those Devices.
DRM Agent	The entity in the Device that manages Permissions for Media Objects on the Device.
DRM Message	A message containing a Media Object and optionally, a Rights Object. Media objects received inside a DRM Message must not leave the Device. The optional Rights Object defines Permissions for the Media Object.
Enable	To make a resource (Media Object) capable of being interacted with. When applied to a digital resource, Enable results in a change in an existing resource such that it becomes capable of being read, written to or executed. Enabling MAY be partial and/or contextual.
Execute	To execute a software programme.
Forward Lock	A special case of the Combined Delivery method where the DRM Message includes only the Media Object and not a Rights Object at all. The Protected Content can be used with all Permissions appropriate to the content type and device capabilities and no Constraints except that the Protected Content is not allowed to be transmitted outside of the Authorised Device.
HTTP Based Adaptive Streaming	Describes a technique where a client can request chunks of an encoded video file by issuing an HTTP GET command to a streaming server. The server hold differently encoded chunks for the same video that are aligned in time and length. The client can choose of which encoding the requested chunks shall be and it can play subsequent chunks of different encoding without interruption of the user experience.

Integrity	The property that data has not been altered or destroyed in an unauthorised manner. (ISO 7498-2)
Media Object	A digital work e.g. a ringing tone, a screen saver, a Java game or a Composite Object.
Network Service Provider	The entity providing network connectivity for a mobile Device.
Network Store	An entity remote to the device and controlled by a service provider which can store DRM Content and encrypted Rights Objects on behalf of a Device for Backup.
OMA DRM Conformant Device	A Device that will work interoperably with other OMA DRM Conformant Devices and some or all of the following; Billing Service Providers, Content Providers and Network Service Providers. It will also Enable DRM Content on the Device only if the Device possesses a valid Rights Object (or implied Rights Object i.e. forward lock) for that instance of DRM Content and only according to the Permissions defined in the Rights Object for that instance of DRM Content.
Overlay	A technique whereby advertisement content is merged with associated DRM protected content such that they can be displayed simultaneously.
Permission	Actual usages or activities allowed (by the Rights Issuer) over DRM Content.
Play	To create a transient, perceivable rendition of a resource.
Print	To create a fixed and directly perceivable rendition of a resource.
Profile Information	Information about the User used to personalise advertisements.
DRM Content	Media Objects that are consumed according to a set of Permissions in a Rights Object.
Restore	Defines an action for duplicating a Media Object and/or Rights Object, transferring it back to the Device from which it was Backed up and then deleting the Rights Object from the backup location if applicable.
Revoke	A Device has been Revoked by a particular Rights Issuers if that Rights Issuers has decided it does not wish to issue Rights Objects to that Device (for example, because it has concerns about the robustness of the Device's implementation).
Rights Issuer	An entity that issues Rights Objects to OMA DRM Conformant Devices.
Rights Object	A collection of Permissions, Constraints and other attributes which define under what circumstances access is granted to, and what usages are defined for, DRM Content. All Authorized Devices must adhere to the Rights Object associated with DRM content.
Separate Delivery	A Version 1 method for delivering DRM Content and Rights Object. The Rights Object and DRM Content are delivered separately, over different transport mechanisms.
Superdistribution	A mechanism that (1) allows a User to distribute DRM Content to other Devices through potentially insecure channels and (2) enables the User of that Device to obtain a Rights Object for the superdistributed DRM Content.
Transfer	To relocate DRM Content or a Rights Object from one place to another.
Unprotected Content	Content which is not DRM Content.
User	The human user of a Device. The User does not necessarily own the Device.

3.3 Abbreviations

3GPP	3rd Generation Partnership Project
CD	Compact Disc
CEK	Content Encryption Key
DRM	Digital Rights Management
DVD	Digital Versatile Disc
HTTP	HyperText Transfer Protocol
ISO	International Standards Organisation
LAN	Local Area Network
MMS	Multimedia Messaging Service

MPEG	Moving Picture Expert Group
MP3	MPEG audio layer 3; coding scheme for audio compression
OMA	Open Mobile Alliance
OS	Operating System
PC	Personal Computer
PDA	Personal Digital Assistant
(P)DCF	(Packetized) DRM Content Format
RFC	Request For Comments
SCR	Static Conformance Requirement
SIM	Subscriber Identity Module
SMS	Short Messaging Service
URI	Uniform Resource Indicator

4. Introduction

(Informative)

Digital Rights Management (DRM) enables the consumption by Users of protected content by allowing Content Providers to express Permissions, e.g., the ability to preview DRM Content, and by specifying how Devices should observe these Permissions.

4.1 Version 2.2

DRM v.2.2 is based on the previous versions of DRM Version 2 & 2.1. Requirements introduced in this version are marked as “DRM 2.2” in the Enabler Release column in Section 6 and Section 7.

5. DRM 2.2 release description (Informative)

This requirements specification document builds on the work in the Version 1 DRM specifications and in total provides:

- The scenarios that we wish to enable with Version 2, 2.1 & 2.2 (Appendix B and Appendix C)
- The high level market requirements derived from the scenarios (section 6)
- The security requirements applying to the technical solution (section 7.1)
- The charging requirements applying to the technical solution (section 7.2)
- The requirements relating to streaming applying to the technical solution (section 7.3)
- The requirements relating to superdistribution applying to the technical solution (section 0)
- The requirements relating to storage and back up of rights and content applying to the technical solution (section 0)
- The requirements relating to rights applying to the technical solution (section 7.6)
- The requirements relating to User privacy applying to the technical solution (section 7.8)
- The requirements relating to terminals and smartcards (that are not covered implicitly or explicitly elsewhere in the document) applying to the technical solution (section 7.11)
- The requirements relating to usability applying to the technical solution (section 7.14)
- The requirements relating to content format applying to the technical solution (section 7.15)
- The requirements relating to interoperability and backwards compatibility applying to the technical solution (section 7.16)

6. Market Requirements

Label	Description	Enabler Release
REQ-MARKT-1	It SHALL be possible to precisely identify DRM Content such that Rights Object may be unambiguously associated with it.	DRM 1.0
REQ-MARKT-2	It SHALL be possible for Rights Issuers to send Rights Objects to Devices	DRM 1.0
REQ-MARKT-3	The Permissions in a Rights Object SHALL be enforced by an OMA DRM Conformant Device.	DRM 1.0
REQ-MARKT-4	It SHALL NOT be possible for a DRM Agent to use DRM Content unless appropriate Rights Object have been associated with that DRM Content and the DRM Agent possesses the required Rights Object	DRM 1.0
REQ-MARKT-5	It SHALL be possible to separate Rights Object and DRM Content physically, but not logically.	DRM 1.0
REQ-MARKT-6	It SHALL be possible for Rights Objects and DRM Content to be delivered via the same or different transport mechanisms. Delivery SHALL be possible using any transport mechanism.	DRM 1.0
REQ-MARKT-7	DRM Content may contain Media Objects of any Content Type.	DRM 1.0
REQ-MARKT-8	It SHALL be possible for the Device to identify whether it can play a certain item of DRM Content before requesting the Rights Object for that item of DRM Content.	DRM 1.0
REQ-MARKT-9	It SHALL be possible for a Rights Issuer to discover whether a Device can play a certain item of DRM Content before issuing the Rights Object (for that item of DRM Content) to the Device.	DRM 1.0
REQ-MARKT-10	<p>Permissions within the Rights Object SHALL enable the following capabilities. All Permissions SHALL be explicitly stated:</p> <ul style="list-style-type: none"> a. It SHALL be possible to specify Permissions for the following rendering types: <ul style="list-style-type: none"> i. Play ii. Execute iii. Display iv. Print b. It SHALL be possible to specify the following Constraints on usage: <ul style="list-style-type: none"> i. Time/date based ii. Count based 	DRM 1.0

REQ-MARKT-11	<p>Permissions within the Rights Object SHALL enable the following capabilities. All Permissions SHALL be explicitly stated:</p> <ul style="list-style-type: none"> c. It SHALL be possible to export both Rights Objects and DRM Content from a Device to another DRM system, to transfer to a copy protected storage medium or to stream over a copy protected transport mechanism. d. It SHALL be possible to specify the following Constraints on usage: <ul style="list-style-type: none"> i. Metered time based (i.e. that the Device can Play the DRM Content as long as the metered usage time is less than a specified time) ii. User identity based (i.e. that the Device can only Play the DRM Content when being used by a specified User) 	DRM 2.0
REQ-MARKT-12	It SHALL be possible to Backup both DRM Content and stateless Rights Objects from a Device.	DRM 2.0
REQ-MARKT-13	It SHALL be possible for the Rights Issuer to reliably identify the Device for the purpose of either issuing or refusing a Rights Object to that Device	DRM 2.0
REQ-MARKT-14	It SHALL be possible for Rights Issuers to protect Rights Objects intended for a particular Device such that the Rights Object can only be processed by that Device.	DRM 2.0
REQ-MARKT-15	It SHALL be possible for Rights Issuers to protect Rights Objects intended for a particular group of Devices (a “domain”) such that the Rights Object can only be processed by Devices within the intended group.	DRM 2.0
REQ-MARKT-16	It SHALL be possible for Devices to send Rights Objects to other Devices (the receiving Device will only be able to process the rights object if the Rights Issuer that issued the Rights Object enables this).	DRM 2.0
REQ-MARKT-17	It SHALL be possible for Rights Objects and DRM Content to be delivered at the same or different times and to be received in any order.	DRM 2.0
REQ-MARKT-18	It SHALL be possible for a Device which receives super-distributed DRM Content to be able to validate its integrity	DRM 2.0
REQ-MARKT-19	It SHALL be possible to package multiple items of DRM Content and download this package to a user, whilst assigning different Permissions for each item of that Composite Object.	DRM 2.0
REQ-MARKT-20	Devices that support the requirements of Version 2 SHALL also comply with all SCR for Version 1 in an interoperable manner.	DRM 2.0
REQ-MARKT-21	It SHALL be possible for a Device to play DRM Content which has been restored from a Backup.	DRM 2.0
REQ-MARKT-22	It SHALL be possible for the Device to copy DRM Content and encrypted Rights Objects to another Device, that does not necessarily have network access e.g. from a phone to a portable media player.	DRM 2.0
REQ-MARKT-23	It SHALL be possible for the RI to enable/disable metering by a specific DRM Agent	DRM 2.1
REQ-MARKT-24	It SHALL be possible for the DRM Agent to record detailed usage data for metered content, including the number of plays and accumulated time consumed.	DRM 2.1
REQ-MARKT-25	It SHALL be possible for the DRM agent to report aggregated usage data for a specific time period to the RI in response to a request from the RI.	DRM 2.1

REQ-MARKT-26	A mechanism SHALL be provided for to allow the DRM Agent to periodically report aggregated usage data for a specific time period to the RI according to a pre-defined RI schedule.	DRM 2.1
REQ-MARKT-27	A mechanism SHALL be provided to enable metering both on Connected and Unconnected Devices.	DRM 2.1
REQ-MARKT-28	The RI SHALL be able to specify the desired behaviour for the case where the DRM Agent does not report back at the requested time. e.g. report at first available opportunity, delay report until next scheduled report date/time. It should also be possible to disable access to metered content until a delayed report is made.	DRM 2.1
REQ-MARKT-29	On withdrawal of user consent to metering the DRM agent SHALL make a metering report to the RI with the final usage information. A final report SHOULD also be made when the user requests an action which will prevent further reporting, e.g. removal of the RI context.	DRM 2.1
REQ-MARKT-30	It SHALL be possible for the RI to configure the period of time (or other suitable metric) that constitutes a consumption for the purpose of metering on a per RO basis i.e. if metered content is consumed for greater than this period of time (or other metric) the DRM Agent will record the consumption as a metered event. If the metered content is consumed for less than this period of time (or other metric) the DRM Agent will NOT record the consumption as a metered event.	DRM 2.1
REQ-MARKT-31	It SHALL be possible for the DRM Agent to inform the RI that some aggregated metering usage data is available for upload.	DRM 2.1
REQ-MARKT-32	ROAP Triggers SHALL support a compact binary encoding scheme.	DRM 2.1
REQ-MARKT-33	It SHALL be possible to use different file extensions to give a basic indication of the type of content e.g. music, video.	DRM 2.1
REQ-MARKT-34	It SHALL be possible for Users and Devices to add to and edit the metadata associated with DRM Content.	DRM 2.1
REQ-MARKT-35	It SHALL be possible for the DRM Agent to confirm installation of an RO to the RI.	DRM 2.1
REQ-MARKT-36	A mechanism SHALL be provided to enable enforcement of advertisement play out before, in between or as part of rendering the DRM Content.	DRM 2.2
REQ-MARKT-37	It SHALL be possible to signal that advertisements cannot be skipped or fast forwarded.	DRM 2.2
REQ-MARKT-38	It SHALL be possible to specify permissions for individual features of DRM content.	DRM 2.2
REQ-MARKT-39	It SHALL be possible for an application to request a license and mitigate error scenarios for content/content features without leaving the application by e.g. opening a browser page. This functionality MAY be provided by an API between DRM Agent and Application.	DRM 2.2
REQ-MARKT-40	It SHALL be possible to issue the certificate for the DRM Agent by an on-line method.	DRM 2.2
REQ-MARKT-41	The profile for the PC certificates SHOULD be defined.	DRM 2.2
REQ-MARKT-42	It SHALL be possible to support HTTP based adaptive streaming of OMA DRM protected content	DRM 2.2
REQ-MARKT-43	It SHALL be possible to specify the number of advertisements that need to be consumed to access the content.	DRM 2.2
REQ-MARKT-44	It SHALL be possible to specify a collection of advertisements, of which one or a subset needs to be consumed to access the content.	DRM 2.2
REQ-MARKT-45	It SHALL be possible for the Device to maintain Profile Information, based on which it can select advertisements to be consumed by the User.	DRM 2.2

REQ-MARKT-46	It SHALL be possible for the Device to dynamically adapt the Profile Information that is used to select advertisements.	DRM 2.2
REQ-MARKT-47	It SHALL be possible for the Server to maintain and dynamically adapt Profile Information that is used to select advertisements.	DRM 2.2
REQ-MARKT-48	It SHALL be possible for the Server and the Device to synchronise the Profile Information for advertisements between the Device and the Server.	DRM 2.2
REQ-MARKT-49	It SHALL be possible for the Device to measure the Advertisement Impression Data.	DRM 2.2
REQ-MARKT-50	It SHALL be possible to control the access to the DRM protected content using the Advertisement Impression Data.	DRM 2.2
REQ-MARKT-51	It SHALL be possible for the RI to generate the Rights Object using the Advertisement Impression Data that was received from the Advertisement Server.	DRM 2.2
REQ-MARKT-52	It SHALL be possible to dynamically update the advertisements needed to be consumed to access the DRM protected content.	DRM 2.2
REQ-MARKT-53	It SHALL be possible to control whether the enforced advertisements are played or not for the same content.	DRM 2.2
REQ-MARKT-54	It SHALL be possible to play different sorts of enforced advertisements for different User for the same content.	DRM 2.2
REQ-MARKT-55	It is the Content Provider to decide which sort of advertisement can be added to the content.	DRM 2.2
REQ-MARKT-56	The enforced advertisements are available for streaming or content download while OMA DRM will not mandate the streaming mechanism.	DRM 2.2
REQ-MARKT-57	It is available to embed the raw advertisements data or link in the content.	DRM 2.2
REQ-MARKT-58	OMA DRM SHALL support mechanisms to Overlay the video with advertisements.	DRM 2.2
REQ-MARKT-59	It SHALL be possible to constrict the number of player devices the User can use to play the content.	DRM 2.2

7. Engineering Requirements

7.1 Security

Label	Description	Enabler Release
REQ-SEC-1	It SHALL be possible for the Confidentiality of the DRM Content to be protected, between the Content Provider and the Device.	DRM 1.0
REQ-SEC-2	<p>The Rights Issuer SHALL be able to authenticate, prior to delivery of Rights Objects to the intended Device, some or all of the following:</p> <ul style="list-style-type: none"> a. The identity of the User of the Device; b. The identity of the subscriber (relating to the Network Service Provider) associated with the Device; c. The identity of the Content Subscription (relating to the Content Provider) associated with the Device; d. The identity of the Device (for example: serial number; Device manufacturer; model number; software version); e. The identity of any smartcard inserted in the Device. <p>Note: Sub-requirement (d) is the only requirement that is explicitly satisfied by the OMA DRM Version 2 specifications.</p>	DRM 2.0
REQ-SEC-3	It SHALL be possible for Rights Issuers to protect Rights Objects for a particular Device or group of Devices such that the Rights Object can only be processed by the intended Device or group of Devices.	DRM 2.0
REQ-SEC-4	The Rights Issuer SHALL be able to conduct the authentication described in requirement (2) of this sub-section without any explicit relationship (contractual or otherwise) with the Device manufacturer.	DRM 2.0
REQ-SEC-5	It SHALL be possible for the Confidentiality of the DRM Content to be protected, in a manner independent of the transport mechanism, between the Content Provider and the DRM Agent on the Device.	DRM 2.0
REQ-SEC-6	It SHALL be possible for the Confidentiality of the DRM Content to be protected, in a manner independent of the transport mechanism, between the DRM Agent on a Device and the DRM Agent on any other Device to which the DRM Content is transferred.	DRM 2.0
REQ-SEC-7	It SHALL be possible for the integrity of the DRM Content to be protected, in a manner independent of the transport mechanism, between the DRM Agent on a Device and the DRM Agent on any other Device to which the DRM Content is transferred.	DRM 2.0
REQ-SEC-8	It SHALL be possible for the Confidentiality of any content encryption key (CEK) in a Rights Object to be protected, in a manner independent of the transport mechanism, between the Content Provider and the DRM Agent on the Device, such that the CEK can only be read by the Device for which the Rights Object is intended.	DRM 2.0
REQ-SEC-9	It SHALL be possible for the Content Provider to encrypt each instance of a particular piece of DRM Content with a different CEK and for superdistribution of that DRM Content to still be possible.	DRM 2.0
REQ-SEC-10	It SHALL be possible for the integrity of the Rights Object to be protected, in a manner independent of the transport mechanism, between the Content Provider and the DRM Agent on the Device for which the Rights Object is intended.	DRM 2.0

REQ-SEC-11	It SHALL be possible for the integrity of the DRM Content to be protected, in a manner independent of the transport mechanism, between the Content Issuer and the DRM Agent on the Device to which the DRM Content is transferred.	DRM 2.0
REQ-SEC-12	It SHALL be possible for the integrity of the Rights Object to be protected, in a manner independent of the transport mechanism, between the DRM Agent on a Device and the DRM Agent on any other Device to which the Rights Object is transferred.	DRM 2.0
REQ-SEC-13	It SHALL be possible for the Confidentiality of any content encryption key (CEK) in a Rights Object to be protected, in a manner independent of the transport mechanism, between the DRM Agent on the Device and the DRM User Agent on any Device to which the Rights Object is transferred, such that the CEK can only be read by Devices for which the Rights Object is intended	DRM 2.0
REQ-SEC-14	It SHALL be possible for the Confidentiality of sensitive information within the Rights Object, for example, user identities, to be protected, in a manner independent of the transport mechanism, between the Content Provider and the DRM Agent on the Device, such that this sensitive information in the Rights Object can only be read by the Device for which the Rights Object is intended.	DRM 2.0
REQ-SEC-15	It SHALL be possible for the Confidentiality of sensitive information within the Rights Object, for example, user identities, to be protected, in a manner independent of the transport mechanism, between the DRM Agent on the Device and any other Device to which the Rights Objects is transferred, such that this sensitive information in the Rights Object can only be read by Devices for which the Rights Object is intended.	DRM 2.0
REQ-SEC-16	It SHALL be possible for the Device to authenticate the identity of the source of the Rights Object.	DRM 2.0
REQ-SEC-17	It SHALL be possible for entities other than the Device manufacturer to provide trusted assertions to Content Providers concerning some or all of the identities listed in requirement (REQ-SEC-2) within this sub-section.	DRM 2.0
REQ-SEC-18	It SHALL be possible for individual components of a composite object to be encrypted with different keys.	DRM 2.0
REQ-SEC-19	It SHALL be possible for some components of a composite object to be encrypted and some not.	DRM 2.0
REQ-SEC-20	It SHALL be possible for the Device time source, as used for DRM purposes, to be protected from interference by the user of the Device or by unauthorized applications loaded onto the Device.	DRM 2.0
REQ-SEC-21	It SHALL be possible for Rights Issuers to synchronize the Device time source, as used for DRM purposes, to a time source within the RI.	DRM 2.0
REQ-SEC-22	It SHALL be possible to encrypt metered usage information so that it can be transferred securely between the OMA DRM agent and the RI.	DRM 2.1
REQ-SEC-23	It SHALL be possible to integrity-protect metered usage information being transferred between the OMA DRM agent and the RI.	DRM 2.1
REQ-SEC-24	If metering is disabled on the user's device (e.g. because the user has not given consent to use metering), the DRM agent SHALL NOT allow rendering of content items which are only accessible using metering	DRM 2.1
REQ-SEC-25	It SHALL be possible to restrict the use of content to a certain class of application.	DRM 2.1
REQ-SEC-26	It SHALL be possible for the Content Issuer and other server entities to reliably identify the DRM Identity(s) of a Device.	DRM 2.1

REQ-SEC-27	It SHALL be possible to protect the integrity of the original metadata (the values set by the Content Issuer).	DRM 2.1
REQ-SEC-28	It SHALL NOT be possible for the DRM Agent to modify the metadata information originally set by Content Issuer. The DRM Agent SHALL store the User-edited metadata information in another place in the (P)DCF.	DRM 2.1
REQ-SEC-29	It SHALL be possible to prevent the user to consume the DRM Content without rendering the Advertisement(s) completely.	DRM 2.2
REQ-SEC-30	It SHALL be possible to restrict access to the DRM protected Content using secure information extracted from the advertisement.	DRM 2.2

7.2 Charging

This sub-section will not specify any particular billing mechanism, merely enablers for billing.

Label	Description	Enabler Release
REQ-CHARG-1	<p>It SHALL be possible for the following charging mechanisms to be supported:</p> <ul style="list-style-type: none"> a. A single Device subscription basis. That is, it SHALL be possible for the Content Provider to deliver to a Device associated with a particular subscription, a defined or unlimited amount of DRM Content with associated Rights Objects over a fixed duration, free of charge, other than the cost of the content subscription. b. A pre-pay basis. That is, it SHALL be possible for the Content Provider to deliver to a Device, an amount of DRM Content with associated Rights Objects, valued up to and including a particular financial sum (which is the current balance of the pre-pay account associated with that Device). c. A per event basis. That is, it SHALL be possible for the Content Provider to deliver to a Device, an item of DRM Content with associated Rights Object and to make a charge for that piece of content as part of the content delivery transaction. 	DRM 1.0

REQ-CHARG-2	<p>It SHALL be possible for the following charging mechanisms to be supported:</p> <ul style="list-style-type: none"> a. A multiple Device subscription basis. That is, it SHALL be possible for the Content Provider to deliver to any subset of a number of Devices associated with a particular subscription, a defined or unlimited amount of DRM Content (with associated Rights Objects) over a fixed duration, free of charge, other than the cost of the content subscription. b. A multiple Device pre-pay basis. That is, it SHALL be possible for the Content Provider to deliver to any subset of a number of Devices associated with a pre-pay account, an amount of DRM Content (with associated Rights Objects) valued up to and including a particular financial sum (which is the current balance of the pre-pay account associated with that collection of Devices). c. A multiple Device per event basis. That is, it SHALL be possible for the Content Provider to deliver to any subset of a specified number of Devices, an item of DRM Content (with associated Rights Object) and to make a charge for that piece of DRM Content as part of the content delivery transaction. 	DRM 2.0
REQ-CHARG-3	It SHALL be possible for a Content Provider to obtain payment from a Billing Service Provider even if the Content Provider and Billing Service Provider are operated by separate organisations.	DRM 2.0

7.3 Streaming

Label	Description	Enabler Release
REQ-STREAM-1	It SHALL be possible to protect the confidentiality of a description of a media streaming session, between the Content Provider and the Device.	DRM 1.0
REQ-STREAM-2	It SHALL be possible to associate a Rights Object with a description of a media streaming session.	DRM 1.0
REQ-STREAM-3	<p>It SHALL be possible to stream (play in real time) DRM Content from the Content Provider to the DRM Agent on a single Device. The requirement applies (but not exclusively) to the following real time protocols :</p> <ul style="list-style-type: none"> a. 3GPP transparent end-to-end packet switched streaming service, see [3GPP PSS] 	DRM 2.0
REQ-STREAM-4	DRM protection of streamed DRM Content SHALL NOT prevent the playing of the DRM Content if there are errors introduced into the content by the transport.	DRM 2.0
REQ-STREAM-5	It SHALL be possible to stream (play in real time) protected content from the Content Provider to a number of DRM Agents on a set of Devices (in both broadcast and multicast modes).	DRM 2.0

REQ-STREAM-6	It SHALL be possible to apply protection between DRM Agents on different Devices to DRM Content that is played in real time such as streaming media. The requirement applies (but not exclusively) to the following real time protocols : <ul style="list-style-type: none"> b. Bluetooth Generic Audio-visual Distribution Profile, [BT GAVDP] c. Bluetooth Audio-visual Distribution Transport Protocol, [BT AVDTP] d. Bluetooth Generic Audio-visual Control Transport Protocol, [BT AVCTP] 	DRM 2.0
REQ-STREAM-7	It SHALL be possible for the RI to restrict access of the Device to an arbitrary chunk of DRM protected multicast media stream.	DRM 2.2
REQ-STREAM-8	It SHALL be possible to protect the confidentiality of a single multicast media stream with multiple encryption keys that are changed sequentially.	DRM 2.2
REQ-STREAM-9	It SHALL be possible to use OMA DRM protection with adaptive HTTP based streaming protocols.	DRM 2.2

7.4 Superdistribution

Label	Description	Enabler Release
REQ-DIS-1	It SHALL be possible for Devices to send DRM Content to other Devices in a transport independent manner, and for Devices receiving DRM Content in such a manner to be able to obtain the Rights Object corresponding to the received DRM Content.	DRM 1.0
REQ-DIS-2	It SHALL be possible for a Device which has received DRM Content from another Device to find out if the DRM Content can be played on the Device before obtaining a Rights Objects for that DRM Content.	DRM 1.0
REQ-DIS-3	It SHALL be possible to use the same download mechanism for the acquisition of a Rights Object as for the acquisition of the DRM Content and the Rights Object from a Content Provider in order to enable the same user experience.	DRM 1.0

7.5 Storage and Backup

Label	Description	Enabler Release
REQ-BCKUP-1	It SHALL be possible for the Device to Backup and Restore DRM Content.	DRM 1.0
REQ-BCKUP-2	It SHALL be possible for the Device to Backup stateless Rights Objects.	DRM 2.0
REQ-BCKUP-3	It SHALL only be possible to Restore Backed up stateless Rights Objects to the Device for which the Rights Object were originally issued.	DRM 2.0
REG- BCKUP -4	.It SHALL be possible for a Device to upload RO(s) to the issuing RI and then the uploaded RO(s) can be restored to another Device belonging to the same User. It SHALL be possible for RI to restore the current state information to the other Device if the RO is stateful.	DRM 2.1

7.6 Rights

Label	Description	Enabler Release
REQ-RO-1	It SHALL be possible to specify Rights Objects for any content type.	DRM 1.0
REQ-RO-2	It SHALL be possible to specify Rights Objects for encrypted and unencrypted content.	DRM 1.0
REQ-RO-3	It SHALL be possible to specify Rights Objects to enable the following rendering types: <ul style="list-style-type: none"> a. Play b. Execute c. Display d. Print 	DRM 1.0
REQ-RO-4	It SHALL be possible to specify Rights Objects containing the following Constraints on usage <ul style="list-style-type: none"> Time/date based Count based 	DRM 1.0
REQ-RO-5	It SHALL be possible to specify content identities within Rights Objects using standard identification schemes. In particular it SHALL be possible to support the use of: <ul style="list-style-type: none"> URI (RFC 2396) 	DRM 1.0
REQ-RO-6	It SHALL be possible to specify Rights Objects containing the metered usage time constraints on usage, for example, it SHALL be possible to specify that the Device can Play the DRM Content as long as the metered usage time is less than the specified time.	DRM 2.0
REQ-RO-7	It SHALL be possible to specify that the Rights Object is bound to a particular User identity, i.e., that a Device can only Play the DRM Content when being used by that User.	DRM 2.0
REQ-RO-8	It SHALL be possible to specify within the Rights Objects associated with DRM Content whether or not the Rights Object and DRM Content can be exported to another DRM system, and to which DRM systems.	DRM 2.0
REQ-RO-9	It SHALL be possible to specify within the Rights Objects associated with DRM Content whether or not the Rights Object and DRM Content can be transferred to copy protected storage media, and to which copy protected storage media.	DRM 2.0
REQ-RO-10	It SHALL be possible to specify within the Rights Objects associated with DRM Content whether or not the Rights Object and DRM Content can be transferred to a rendering device over a copy protected transport mechanism, and over which copy protected transport mechanisms.	DRM 2.0
REQ-RO-11	It SHALL be possible to specify Rights Objects associated with DRM Content where the DRM Content is a Composite Object.	DRM 2.0
REQ-RO-12	It SHALL be possible to independently specify Rights Objects for each individual component of a Composite Object.	DRM 2.0
REQ-RO-13	It SHALL be possible to specify within the Rights Objects whether or not the associated DRM Content can be exported to another format, including specifying the allowed formats (CD, DVD, "any" etc.) and also the characteristics of the resultant content (e.g. specifying quality parameters like bitrates or "allow all").	DRM 2.1

REQ-RO-14	It SHALL be possible to specify within the Rights Objects associated with DRM Content whether or not the decrypted DRM Content can be transferred over an unsecured path to the rendering device. The path includes player, codec and device drivers.	DRM 2.2
REQ-RO-15	It SHALL be possible to specify within the Rights Objects associated with DRM Content which is the maximum resolution of content to be decrypted.	DRM 2.2
REQ-RO-16	It SHALL be possible to signal that consuming one or a subset from a collection of advertisements is needed to access the content.	DRM 2.2
REQ-RO-17	It SHALL be possible to specify in the Rights Object that advertisement impression data has to be collected.	DRM 2.2
REQ-RO-18	It SHALL be possible to specify in the Rights Object the number of the advertisements required to access the DRM protected content.	DRM 2.2
REQ-RO-19	It SHALL be possible to contain advertisement indication information in the Rights Objects for the enforced advertisements.	DRM 2.2
REQ-RO-20	It SHALL be possible to define how the enforced advertisements will be displayed (Overlay vs. explicit payout).	DRM 2.2
REQ-RO-21	It SHALL be possible to specify Rights Objects containing the Constraints of the number of player devices for the content on usage.	DRM 2.2

7.7 Domains

Label	Description	Enabler Release
REQ-DOM-1	It SHALL be possible for the Rights Issuer to authorise certain Devices to form a domain, such that all the Devices in that domain, and only those Devices, can process Rights Objects intended for that domain.	DRM 2.0
REQ-DOM-2	It SHALL be possible for the Rights Issuer to authorise Devices to join a domain that has already been formed.	DRM 2.0
REQ-DOM-3	It SHALL be possible for the Rights Issuer to direct a Device to leave a domain.	DRM 2.0
REQ-DOM-4	It SHALL be possible for the Rights Issuer to exclude one or more Devices in the domain, such that the excluded Devices cannot process any new Rights Objects issued for the domain after the time of exclusion.	DRM 2.0
REQ-DOM-5	It SHALL be possible for Devices in a domain to leave the domain.	DRM 2.0

7.8 Privacy

Label	Description	Enabler Release
REQ-PRIV-1	User and Device specific information SHALL NOT be disclosed to the Content Provider and/or to other parties without the explicit consent of that User.	DRM 1.0
REQ-PRIV-2	User and Device specific information SHALL NOT be disclosed by the Content Provider to any 3 rd party without the explicit consent of the User.	DRM 1.0
REQ-PRIV-3	It SHALL be possible for Confidentiality to be maintained when User specific information such as the User identity is sent from the Device.	DRM 1.0

REQ-PRIV-4	It SHALL NOT be possible for the RI to enable metering without user consent. It SHALL be possible for the RI to enable metering without requiring the Device to display an explicit user confirmation dialog i.e. The RI may obtain user consent for metering using mechanisms that are outside of the scope of OMA DRM v2.1.	DRM 2.1
REQ-PRIV-5	A DRM Agent SHALL only provide metering information to RIs with which it has a valid RI Context.	DRM 2.1
REQ-PRIV-6	A DRM Agent SHALL only provide metering information to an RI in response to a specific request from the RI or as part of a RI-defined schedule.	DRM 2.1
REQ-PRIV-7	It SHALL be possible for the user to withdraw consent to usage of metering at any time. On withdrawal of user content the DRM agent SHALL NOT record any further usage information and SHALL return a final metering report.	DRM 2.1
REQ-PRIV-8	It shall NOT be possible for an RI to get metering information for ROs he has not issued.	DRM 2.1
REQ-PRIV-9	It SHALL be possible for the User or the Device to select advertisements to be consumed by the user, without contacting/informing a third party (including the RI and Content Issuer).	DRM 2.2
REQ-PRIV-10	It SHALL be possible to signal whether the mechanism from REQ-PRIV-9 is used.	DRM 2.2
REQ-PRIV-11	It SHALL be possible for the user to prevent third party access (including access by the RI and Content Issuer) to the Profile Information from REQ-MARKT-45.	DRM 2.2
REQ-PRIV-12	It SHALL be possible to specify whether the mechanism from REQ-MARKT-48 is used.	DRM 2.2

7.9 Error Handling

Label	Description	Enabler Release
REQ-ERR-01	It SHALL be possible for the RI to request from the DRM Agent information on the current status of the RI context, e.g. <ul style="list-style-type: none"> - against which RI ID it is registered - the ROAP base URL - the domain(s) it has joined 	DRM 2.2
REQ-ERR-02	It SHALL be possible for the RI to request from the DRM Agent the DRM activity log containing <ul style="list-style-type: none"> • triggers that were received via WAP Push • triggers that were downloaded • licenses that were received via WAP Push • ROAP messages that were sent 	DRM 2.2
REQ-ERR-03	It SHALL be possible for the RI to request from the DRM Agent the Domain Name Whitelist (see [DRM-v2.1-DRM-TS])	DRM 2.2
REQ-ERR-04	There DRM Agent SHALL offer an interface to allow applications additional functionality: <ul style="list-style-type: none"> - to trigger license update, - to access DRM protected files, - to retrieve qualified DRM error codes 	DRM 2.2

REQ-ERR-05	A mechanism SHALL be provided a reliable transfer of metering data allowing correct recovery from failures keeping metering data consistent between DRM Agent and server even in cases of system failure or when execution stops (completely or partially)	DRM 2.2
------------	--	---------

7.10 Administration and configuration

No requirements identified.

7.11 Terminal Devices and smartcards

7.11.1 Terminal Devices

Requirements are stated elsewhere in this document.

7.11.2 Smartcards

Label	Description	Enabler Release
REQ-SCARD-1	The Device SHALL be able to use the smart card to provide User identification and authentication when obtaining and verifying Rights Objects.	DRM 1.0

7.11.3 Removable Media Cards

Label	Description	Enabler Release
REQ-MCARD-1	It SHALL not be possible for the Device to move DRM Content protected with either the Forward Lock or Combined Delivery wrapper to a removable media card.	DRM 1.0

7.12 Platforms

No requirements identified.

7.13 Network interfaces

No requirements identified.

7.14 Usability

Label	Description	Enabler Release
REQ-USE-1	It SHALL be possible for the User to delete an instance of DRM Content, but to keep the Rights Objects associated with that content (so that he/she could restore the DRM Content on the Device later without having to obtain new Rights Objects).	DRM 1.0
REQ-USE-2	It SHALL be possible for a User to view a description of the DRM Content without retrieving the Rights Object.	DRM 1.0
REQ-USE-3	It SHALL be possible for the User to view information, e.g. copyright information, available Permissions, regarding Rights Objects on the Device.	DRM 1.0
REQ-USE-4	It SHALL be possible to specify, within the DRM Content, text information provided by the Content Issuer (e.g. title, author, copyrights). This information, if provided, SHALL be available to the User.	DRM 1.0

REQ-USE-5	As far as possible, metering SHALL be transparent to the end user, i.e. there should be minimal interactions with the User.	DRM 2.1
REQ-USE-6	As far as possible, users should not experience lack of access to metered content because of delays in processing metering reports by the RI or other robustness issues.	DRM 2.1

7.15 DRM content

Label	Description	Enabler Release
REQ-DCF-1	It is desirable that DRMv2.1 Devices support the non-streamable PDCF format, therefore it is RECOMMENDED that Devices support the non-streamable PDCF format.	DRM 2.1
REQ-DCF-2	It SHALL be possible for the Content Issuer to include metadata information in the (P)DCF.	DRM 2.1
REQ-DCF-3	It SHALL be possible for the Content Issuer to embed content related data e.g. a cover art picture or lyrics in the (P)DCF, or an URI where the content related data may be retrieved from.	DRM 2.1
REQ-DCF-4	It SHALL be possible for the DRM Agent to store the user-edited metadata information in the (P)DCF.	DRM 2.1
REQ-DCF-5	It SHALL be possible for the DRM Agent to cancel the user edits and revert back to the original metadata information in the (P)DCF.	DRM 2.1
REQ-DCF-6	It SHALL be possible to store Advertisement Content (i.e. one or multiple advertisements) in a multipart DCF with or without the related DRM protected Content.	DRM 2.2
REQ-DCF-7	It SHALL be possible to dynamically update Advertisement Contents stored in the multipart DCF without updating the RO of the associated DRM content.	DRM 2.2
REQ-DCF-8	It SHALL be possible to add metadata to advertisements, such that the metadata can be used by the Device to select advertisements to be consumed by the user.	DRM 2.2
REQ-DCF-9	It SHALL be possible to signal an expiry date for advertisements.	DRM 2.2
REQ-DCF-10	It SHALL be possible to deliver advertisements as part of the DRM content itself.	DRM 2.2
REQ-DCF-11	It SHALL be possible to contain advertisement indication information in the (P)DCF format for the enforced advertisements.	DRM 2.2
REQ-DCF-12	It SHALL be possible to contain raw data of the enforced advertisements in the (P)DCF format.	DRM 2.2

7.16 Interoperability and backward compatibility

Label	Description	Enabler Release
REQ-IOP-1	Devices that support the requirements of Version 2 SHALL also comply with all SCR for Version 1 in an interoperable manner.	DRM 2.0
REQ-IOP-2	The supported DRM version SHOULD be exposed.	DRM 2.0

REQ-IOP-3	It SHALL be possible to use the AES_128_BYTE_CTR encryption method from [XBS-v1.0] in PDCF.	DRM 2.2
REQ-IOP-4	It SHALL be possible to use the Short Term Key Message tracks from [XBS-v1.0] in PDCF	DRM 2.2

Appendix A. Change History

(Informative)

A.1 Approved Version History

Reference	Date	Description
OMA-RD-DRM-V2_1-20081014-A	14 Oct 2008	Status changed to Candidate by TP ref# OMA-TP-2008-0382-INP_DRM_V2_1_ERP_for_Final_Approval

A.2 Draft/Candidate Version DRM 2.2 History

<< Document Identifier	Date	Sections	Description
Draft Versions OMA-RD-DRM-V2_2	08 Oct 2009	N/A	Incorporates input to committee: OMA-DRM-2009-0198R01-INP_RD_DRM_V2_2.zip RD Template 2009
Draft Versions OMA-RD-DRM-V2_2	17 Jan 2010	N/A	Incorporates input to committee: OMA-DRM-2009-0243r01-CR_DRM_2.2_RD_Usecase_for_Advertisemen OMA-DRM-2009-0215R01- CR_DRM22_Requirements_for_Ad_Managemen OMA-DRM-2009-0200-CR_DRM22_Requirements_for_PDCF
Draft Versions OMA-RD-DRM-V2_2	08 Feb 2010	N/A	Incorporates input to committee: OMA-DRM-2010-0008- CR_Usecase_for_Secure_streaming_support_with_variable_bitratesOMA- DRM-2010-0009R01- CR_Requirements_for_Secure_streaming_support_with_variable_bitrates OMA-DRM-2010-0019-CR_DRM2.2_Clerical_changes_to_Usecase_24 OMA-DRM-2010-0021R01-CR_New_scenario_for_secure_streaming OMA-DRM-2010-0022R01- CR_DRM_2.2_RD_for_Games_and_Executables OMA-DRM-2010-0023R01-CR_personalized_advertisement_for_user OMA-DRM-2010-0024R01- CR_personalized_advertisement_for_domain_user OMA-DRM-2010-0026R01-CR_DRM_2.2_RD_Enhanced_Error_Handling OMA-DRM-2010-0029R03-CR_DRMv2.2_RD_Dynamic_Ad_Update OMA-DRM-2010-0033R01-CR_DRMv2.2_RD_PC_Platform_Support OMA-DRM-2010-0035- CR_DRM22_Usecase_for_personalised_advertisements OMA-DRM-2010-0059R01-CR_DRM_2.2_RD_Scope_Clarification OMA-DRM-2010-0060R01- CR_DRM_RD_2.2_Definition_of_Term_Overlay OMA-DRM-2010-0061R03- CR_DRM22_Collected_requirements_for_advertisements
Draft Versions OMA-RD-DRM-V2_2	11 Feb 2010	N/A	Incorporates input to committee: OMA-DRM-2009-0244R03- CR_DRM_2.2_RD_Requirements_for_Advertisement OMA-DRM-2009-0245- CR_DRM_2.2_RD_Usecase_for_PlayerDevice_Number_Restriction OMA-DRM-2009-0246r01- CR_DRM_2.2_RD_Requirements_for_PlayerDevice_Number_Restriction OMA-DRM-2010-0011R01- CR_Usecases_for_two_Advertisements_models
Draft Versions OMA-RD-DRM-V2_2	24 Mar 2010	N/A	Editorial Cleaning up Updated with the RD 2010 Template
Draft Versions OMA-RD-DRM-V2_2	06 May 2010	N/A	Incorporated the following agreed CRs: OMA-DRM-2010-0086R03-CR_RD_definition_of_User_Profile OMA-DRM-2010-0115R01-CR_DRM22_RD_usage_scenarios

<< Document Identifier	Date	Sections	Description
Draft Versions OMA-RD-DRM-V2_2	31 May 2010	N/A	Incorporated the following agreed CR: OMA-DRM-2010-0126-CR_Clerical_Changes
Candidate Version OMA-RD-DRM-V2_2-20100629-C	29 June 2010	N/A	Status changed to Candidate by TP # OMA-TP-2010-0249-INP_DRM_V2_2_RD_for_Candidate_Approval

Appendix B. Use cases (Informative)

This section describes the new use cases enabled by DRM2.2. For a description of the legacy usage scenarios covered by DRM2.1, please see Appendix C.

B.1 Enforced advertisement playback

B.1.1 Short Description

Miss Li is an undergraduate student. When she goes to purchase a season of her favourite comedy show, two options show up in the webpage. One option is for the show without advertisement at a higher price; the other one is for the show with advertisements at a lower price.

The Advertisements are provided by the SP. The type of advertisements to be shown can depend on Miss Li's profile which can be based on her personal preferences, or on previous content consumed, or on the demographic of Miss Li such as age. In this case, Miss Li is a sports fan, and chooses to buy the season of the show at a lower cost with sports related advertisements. She is shown an advertisement about an important game coming up, and decides to buy tickets to watch the game.

The content and/or the Rights Object may contain the information to indicate the terminal to play the selected advertisements before the content play or at a middle slot during the content play and the enforced advertisements can not be skipped, so viewing of the rest of the contents is not possible until advertisement is played out. The advertisement content may be subsequently dynamically updated by the advertising agency, for example to be seen on subsequent viewings.

Alternative cases

- (a) Miss Li can be given the option to select the amount of advertisements to view, which will affect the cost. For example, she selects the show which has a cost of \$20 without advertisements. If she selects 3 advertisements, the price of the show is \$15. If she selects 1 advertisement, the price is \$19.
- (b) Miss Li may buy the show with 3 advertisements which has rights extending across a domain of users, including herself and her friend Bob. In this case, the restriction (i.e. watch 3 advertisements) applies across all users in the domain, however the advertisements to be shown will be personalised differently for Miss Li and Bob.
- (c) Miss Li has previously agreed with the content provider that she always wants adverts, so she is not shown the options on the webpage.
- (d) Miss Li purchases a game service, where she can play a game 5 times once the advertisements associated to the game are watched.
- (e) In some cases, the rendering of selected advertisements may even replace the need for Miss Li to pay for the associated content.

B.1.2 Market benefits

Benefit to customer is reduced cost of content.

Benefit to advertising agency is more opportunities to reach the customer.

B.2 Purchase within an application

B.2.1 Short Description

Tom buys a new handset that was offered as a Game Bundle. The handset already contains a set of games that can be played in trial mode. Tom starts playing a Tetris game.

He can play for free until he reaches level 3. The application asks him if he wants to purchase a full license for 1\$ so that he can continue. Tom confirms. The Games backend triggers license delivery e.g. by sending a WAP Push Trigger. Tom's handset downloads the rights object. Tom's handset receives a rights object allowing Tom to play the game he has selected without any further restrictions. Tom can now continue to play the game

Alternative cases:

1. (a) The application asks Tom if he would like to purchase the option to play online against other players, if he purchases the multiplayer mode for an additional 1\$.

B.2.2 Market benefits

Benefit to customer to trial a limited version of game for low cost.

Benefit to game provider of option of additional revenue streams.

Benefit to operator to enable pre-installation of games, with subsequent revenue streams but minimal network load for downloads.

B.3 Variable bitrates streaming

B.3.1 Short Description

Jo has a subscription for a Video on Demand service that offers "streaming" of movies to PC and handset. The subscription service uses OMA DRM to ensure that no unprotected streamed content can be captured but can only be viewed during a valid subscription. Jo starts watching a movie on her smart phone while sitting in a train. Jo starts watching the movie in the native resolution of her smartphone.

As the train passes the countryside, the available bandwidth decreases and does not support the bandwidth required for native resolution any more. Still, the movie goes on playing on Jo's smartphone without frame drops or pauses as the smartphone now uses a version of the movie encoded with lower resolution.

Passing an area with better network coverage, the available bandwidth increases. Without any interaction, the smartphone now uses a version of the movie encoded in the optimal resolution for her phone.

B.3.2 Market benefits

Improved experience for customer, as their movie is watched uninterrupted.

B.4 Video streaming: maximum resolution & secure path

B.4.1 Short Description

Jo has a subscription for a Video on Demand service that offers "streaming" of movies to PC and handset. She has signed a subscription for standard definition content.

Jo is using a PC as a video server for her home entertainment system. She chooses a movie from the subscription service. Despite the fact that the movie is available in HD, the DRM license on her PC only allows for standard definition, so the movie is downloaded from the subscription service in an SD encoding.

Alternative use cases:

(a) the DRM license only allows encrypted digital output, but no unprotected analogue output. Hence Jo can watch the movie on her TV which is connected using the HDMI port, but is not able to record the content onto DVD since the DVD recorder is connected via a SCART connector providing an analogue RGB signal.

(b) the rights object requires that the content is only sent to the digital output via a secured path. Hence Jo can watch the content on her TV via her PC, as her PC fulfils this requirement. However a day later Jo is taking her Linux based Netbook with her. The Netbook is in the same DRM domain as her PC, therefore she is entitled to watch the movie. Jo can watch the movie on the built-in display of her Netbook, but she cannot watch it on a HD TV set attached to the Netbook, because it does not provide a secure path to the TV set.

B.4.2 Market benefits

Supports differential charging models for SD and HD content.

Protects against indiscriminate copying of content via unprotected outputs.

B.5 Restriction on number of Player devices

B.5.1 Short Description

The SP provides a service option for the content consuming that the number of Player Devices be considered in the price of content.

Mr. Tan only has two personal devices, so he purchases a piece of content with the restriction within two Player Devices and with 10 times Move permission.

Once Mr. Tan has ever played the content in his two devices, the content will not be able to be played in another third device. If still remains some Move count permissions, the content can only be played between these two devices.

B.5.2 Market benefits

Enables price plans based on allowed number of player devices.

Appendix C. DRM 2.1 usage scenarios (Informative)

This section is intended to describe in the form of user scenarios the types of services which customers will require when they come to have access to a wider range of content. The scenarios are based upon a student although many of the principles will apply to older users and potentially to younger ones as well. The examples given try not to relate to any particular mobile operator, Content Provider or Device manufacturer (although several are mentioned) and are given to help understand the actual way in which users MAY want to deal with content distributed to mobile Devices in the future. Some of the user cases MAY be seen as being too difficult or MAY mandate a particular business model. This is not intentional and MAY lead to the scenarios changing to reflect an easier solution or an enlarged business solution.

Simply, the purpose of this section is:

1. To provide a better understanding of the functionality that the OMA DRM Version 2 solution should provide.
2. To offer high level descriptions of different OMA scenarios against which the formal requirements for OMA-DRM Version 2 can be checked
3. To be a public document that can help to explain what OMA-DRM Version 2 is about.

This section describes the usage scenarios (a precursor to use cases) covered by DRM2.1. For the new use cases covered by DRM2.2, please see Appendix B,

Jo is an active teenager in 2003. She has many friends both in her real and virtual worlds. She belongs to several virtual communities and likes to share experiences with them. Her friends in her real world enjoy interacting socially when they meet and also using other messaging techniques such as email, instant messaging and even short messaging when they cannot talk.

Jo owns a range of different electronic Devices including a digital camera that can take still pictures and short video clips. She has in effect become a Content Provider herself and would like to be able to control the content which she sends both to her friends and that she places onto a personalised web site.

The other Devices that she owns have a range of communications mechanisms including Bluetooth and wireless LAN. Her iMac has Bluetooth connectivity, her PDA is Bluetooth enabled, her tablet PC which she uses to take notes in lectures is connected with 802.11 technology. Some Devices MAY have network connectivity built into them (e.g. mobile phone), some MAY have intermittent connectivity (e.g. a PDA with Bluetooth) and some MAY never have any connectivity with the network (e.g. an MP3 player).

She owns a number of CDs and DVDs with content from well-known record and film companies.

She has subscriptions with several Content Providers, both her mobile operator and Internet-based Content Providers, which enables her to download and stream songs to her PC and mobile Devices.

Note: Discussions regarding content types are for example only. Other content types MAY be considered.

In the user cases described below, it is important to note that the facilities offered to Jo and her friends are made only if appropriate Rights Objects have been specified by the Content Provider, allowing her to do this.

Scenario 1 - Using content on multiple devices

Jo purchases and downloads a protected music track to her mobile phone. She sends a copy of the track to her DRM compliant portable music player by:

- a. using a Bluetooth connection with the player, or
- b. copying the track to a removable memory card, and moving the card to her music player.

Jo can listen to the track on both her phone and on the music player. She can do this because when she bought the track, she agreed to a purchase agreement on the transaction, which explicitly allows her to use the track on another, specified OMA DRM Conformant Device. However, depending on the purchase agreement, she may only be able to listen to the track on one of devices at one time, or may be able to listen to the tracks on both devices at the same time.

Scenario 2 - Buying Rights Objects for another user

Jo hears about a great song and wants to send it to her mother. She uses a service from her Rights Issuer to buy the Rights Object to the song for her mother and enables her mother to receive the content (and Rights Object) on her Device and play the song.

Scenario 3 - Restoration of Rights Object and content using a secure portable user identity

Jo drops her mobile Device resulting in a catastrophic failure, she calls her Network Service Provider who replaces the Device (under her insurance agreement). The embedded portable smartcard Device carries her identity in a secure way. The smartcard has not been damaged and she is able to insert it in the replacement Device and use this as an authenticated identity which allows her to download the DRM Content and Rights Object previously purchased from the Content Providers.

Scenario 4 - Backup of DRM Content and Rights Object from a Service Provider

Jo loses her mobile Device which contains many DRM Content files and related Rights Object. She calls her Network Service Provider who replaces the Device (under her insurance agreement). The Device is only set up to her default subscription. Luckily, her Content Provider maintains a record of the content which Jo owns, and she is able to login to her Content Provider who automatically downloads the DRM Content and related Rights Object which she has previously purchased to her new Device.

There is no specified method of storing information relating to the state of stateful Rights Objects outside the Device to which the Rights Objects apply.

The Rights Issuer can Revoke the old Device (preventing it from future access to OMA DRM services) to prevent possible fraud.

Scenario 5 - Local Device Backup of content and Rights Object

Jo has a mobile Device with a removable media slot. She makes a Backup of her Media Objects and stateless Rights Objects, which she has previously purchased, on a removable media, and leaves it at home. Then Jo drops her mobile Device resulting in a catastrophic failure, she calls her Network Service Provider who replaces the Device (under her insurance agreement). The removable media is safe, so she is able to insert it in the replacement Device, restore all the objects to the Device and continue to use the Media Objects once new Rights Objects have been re-issued to the replacement Device. She cannot restore the stateless Rights Objects on the new Device, as the Rights Objects could only have been restored to the old Device.

The Rights Issuer can Revoke the old Device (preventing it from future access to OMA DRM services) to prevent possible fraud.

Scenario 6 - Protecting user generated content

Jo would like to create content (photo etc.) and send it to her friend. However, she does not wish her friend to forward it to anybody else. Her Device provides the capability to give her content a "forward lock". The transport for her content is unspecified, but could be MMS.

Scenario 7 - Export of DRM Content and Rights Objects to other DRM systems and/or transfer to copy-protected storage medium/transport

Jo purchases and downloads an OMA DRM protected music track to her mobile phone. She plays the music on her mobile phone for several days, and then decides she would prefer to play it on another music player that has a different DRM protection format.

Jo can choose between the following mechanisms to render the track on a different player. In all cases, the Content Provider can specify whether the alternative rendering mechanism is allowed or not.

1. She exports the music and its Rights Object (or its equivalent in the exported-to DRM) to the other player using a Bluetooth connection or via removable media. Now she cannot play the music on her mobile phone but can play it on the other DRM-compliant music player.
2. She transfers the music track to a copy protected storage medium. Jo can now play the track on any player that supports this storage medium. The copy protection mechanism of the storage medium prevents copying of the tracks from the medium.

3. She streams the music tracks from her mobile phone to a rendering device for immediate playback. An example of such a rendering device is a headphone. The transmission protocol between her mobile phone and the rendering device incorporates copy protection so that the track cannot be copied.

Scenario 8 - Multiple Contents Scenario

Jo subscribes to a music service where she can download favourite songs for karaoke. Each karaoke song is delivered as a package that includes the music and lyrics for the song as well as associated images and links to related content. She can play and sing the songs with her mobile karaoke player. A single Rights Object for this package can specify different Permissions for the individual components. The content provider wants to promote the song so it allows the lyrics, images, and other information to be copied for free so Jo can share them with her friends. Through this promotion, the content provider hopes to stimulate sales of the music.

The package of music, lyrics and pictures might be sent by MMS.

Although the package contains several parts, Jo may only have a single Rights Object associated with that content package.

Scenario 9 - Basic download

Jo browses a content provider's portal and decides to acquire downloadable content. She completes the required browsing, ordering and payment transactions. She downloads the content object to her Device and receives the Rights Object that is sent to her Device, and is subsequently able to play the content subject to the terms described in the Rights Object. The content is protected against use or misuse that does not comply with the Rights Object set by the Content Provider.

The types of Permission she may have are:

- Time based Rights Object allowing her to listen to the song until a particular date.
- Metered usage time based rights allowing her to listen to the song as long as the metered usage time is less than a specified time, whilst ensuring that she cannot alter the accumulated time to give herself additional usage.

Scenario 10 - Subscription

Jo has subscribed to an Internet music service that she accesses through her mobile Device. The mobile Device has removable storage and music playing capability. The service allows Jo:

- Music streaming to her mobile Device for on-demand listening with play control (pause, resume, etc.).
- Music download to her mobile Device. The music can be listened to, as long as the subscription is active (even when the Device is out of coverage), either when the Device is connected to or disconnected from the Internet site.

Scenario 11 - Basic streaming

Jo browses a Content Provider's portal and decides to see an audiovisual stream showing a concert of her favourite group. She completes the required browsing, ordering and payment transactions. She downloads some information for the streaming player to her Device and receives the Rights Object. The Rights Object describes Jo's Permissions concerning setting up, receiving and playing the streams. She is subsequently able to set up the audio and video streams and play them subject to the terms described in the Rights Object.

Scenario 12 - Multicast streaming under subscription

Jo has a paid subscription with an Internet radio service that she accesses through her mobile Device. The service allows Jo to select one of number of multicast radio channels and listen to the multicast stream on that channel. The music can be listened month after month, as long as the membership is active when the Device is connected to the Internet site.

Scenario 13 - Backwards compatibility

Jo receives many forms of content from various service providers. When her new Device receives content from service providers only utilising the Version 1 DRM mechanism, her new Device handles these requests according to the requirements specified for Version 1 compliant Devices, without causing Jo any problems.

Scenario 14 - Preview Rights Object

Jo receives a music clip of a band she has never heard of before by superdistribution. She is issued preview Rights Object allowing her to listen once to the music, or allowing unlimited playback of a small section of the music before she decides to buy the full set of rights. In the case of allowing unlimited playback of a segment of the file, Jo is able to preview while the remainder of the file is being downloaded. This type of Rights Object may also apply to a clip at the start of streamed data.

The types of possible permissions within the Rights Object that Jo may receive either:

- state that the Media Object can only be played once, or
- describe the starting and finishing times of the free preview clip

Scenario 15 - Superdistribution

Jo has received DRM Content via a local link (e.g. Bluetooth, IrDA ...) from her friend. She wants to acquire Rights Object to get access to that content and follows the appropriate reference provided for that purpose in the DRM Content. Jo explores the offer to obtain new Rights Object. Before Jo is charged for the new Rights Object she expects that

- the integrity of the DRM Content is verified to avoid buying Rights Object for content that isn't usable,
- the properties of the DRM Content are validated to be suitable for Jo's Device,
- the process of acquiring new Rights Object provides the same user experience as the process of purchasing new DRM Content with associated Rights Object.
- the Rights Object issuer has been authenticated.

Scenario 16 - Revoke Device

The Content Provider wishes to prevent Jo from being able to acquire new content for her Device, for example, because Jo has illegally shared her content with friends in the past. The Content Provider therefore revokes Jo's Device and Jo no longer receives DRM Content or Rights Objects from that Content Provider.

Scenario 17 - Binding Rights Objects to User Identity

Jo has two phones but only one SIM – she puts her SIM in the phone she wants to use. Jo has a game that she wants to be able to play on both her phones but does not want to buy it twice. Jo's Rights Issuer therefore issues both of Jo's phones with a Rights Object for the game. The Rights Object is tied to the presence of Jo's SIM so she can only play the game on the phone with her SIM in. When she lends one of her phones to Bob, who puts his SIM in, the Rights Object cannot be used.

Scenario 18 - Basic (silent) auto-renewal of Right Objects

A Rights Object on Jo's mobile phone expires. Jo goes to play the associated DRM Content. Instead of immediately notifying Jo that her Rights Object have expired, the DRM Agent on the phone first contacts to the DRM service provider to request renewal. Only if the Content Provider refuses does the DRM Agent alert Jo that she needs to go and re-acquire Rights Object.

Scenario 19 - Redirection to Rights Issuers from Content Provider

Jo's Rights Object have expired. Jo's mobile Devices attempted to acquire Rights Object from the Content Provider. The Content Provider refuses but returns a message stating that Rights Object can be bought from a named (set of) alternative Rights Issuers. Jo can select the link to initiate a browser connection to one of the Rights Issuers. Jo re-purchases the Rights Object. The chosen Rights Issuer updates the Content Provider of the newly acquired Rights Object.

Scenario 20 - Hacked DRM Solution

OMA DRM solution becomes a very widely adopted DRM standard, and hence becomes the focus of attention for an attempt at cracking the cryptographic implementation.

The Rights Issuer identifies that the Device is insecure, notifies Jo and adds the Device identity (DRM agent, SW version, Device equipment number...) to a black list for DRM Content download.

Scenario 21 - Operation with Varying Cryptographic Strengths

Jo is using a Device which is legally prohibited from using the highest strength ciphers supported by OMA DRM. Content Providers and Rights Issuers are able to discover which ciphers are supported by Jo's Device before sending encrypted data to it.

Scenario 22 - Metered Subscription

A Metered Subscription is a subscription service where the Device returns detailed usage information to the RI for the purpose of Royalty collection. Information has to include the number of times that a specific Media Object has been consumed.

In order to access a wide variety of premium content Jo subscribe to a Metered Subscription service. Once subscribed Jo has access to any content item in the subscription catalogue (while the subscription is still valid). If the content item is metered the rendering action (play, display, execute, print) and number of plays, time rendered or other consumption parameters are recorded by the DRM Agent within the Device. Towards the end of the subscription period the aggregated metering usage information is reported back to the RI by the DRM agent.